RAVEN: A MESSAGING APPLICATION PROTOTYPE FOR PRIVACY UNDER COERCION

Juan Santos Trigo Nasser[1], Fabio Vivarelli[2], João Pedro Veríssimo Gonçalves[3], Ana Paula Abrantes de Castro Shiguemori[4]

[1]Federal Institute of Education, Science and Technology of São Paulo, Jacareí, Brazil (juan.nasser@aluno.ifsp.edu.br)
[2]Federal Institute of Education, Science and Technology of São Paulo, Jacareí, Brazil (fabio.vivarelli@aluno.ifsp.edu.br)
[3]Federal Institute of Education, Science and Technology of São Paulo, Jacareí, Brazil (joao.verissimo@aluno.ifsp.edu.br)
[4]Federal Institute of Education, Science and Technology of São Paulo, Jacareí, Brazil (anapaula.acs@ifsp.edu.br)

Abstract: This paper presents Raven, a messaging application prototype focused on privacy under physical coercion. The prototype combines a primary password, a secondary password that opens a fake environment, and an emergency mode designed to reduce the exposure of sensitive conversations. The local minimum viable product (MVP), developed in Flutter, demonstrates access flows, mock conversations, and security settings, providing a foundation for future cryptographic and backend layers.

Keywords: privacy; physical coercion; secure messaging; plausible deniability; prototype

INTRODUCTION

Digital communication has become central to journalistic work, social organization, and everyday life. In authoritarian contexts, however, the risk is not limited to remote interception (NEWSWEEK, 2026). A user may also face physical coercion, in which an authority or a third party forces the person to unlock a device and show messages, contacts, images, or installed applications. In this scenario, the security problem moves from the network to the device itself, making it insufficient to protect only the communication traffic between users.

A case that illustrates this problem occurred in March 2022, when Anna Vasilyeva, a reporter for the Russian newspaper Kommersant, published footage allegedly showing police officers in Moscow allegedly stopping pedestrians near Lubyanka Square and checking their phones. International reports stated that officers demanded to inspect messages and phone activity, and that people who refused to hand over their phones had difficulty being released (NEWSWEEK, 2022; BUSINESS INSIDER, 2022).

Since then, press freedom organizations have documented additional cases involving journalists in Russia. Svetlana Khustik was detained in 2025 and faces charges of spreading allegedly false information about Russia's full-scale invasion of Ukraine, with a possible sentence of up to ten years (CPJ, 2025a). Sergey Mingazov, a journalist for Forbes Russia, was placed under house arrest in 2024 after reposting information about Bucha, and later received a fine in 2025 (CPJ, 2024a; IPI, 2025). Sergey Mikhaylov, publisher of the independent newspaper Listok, was sentenced to eight years in prison in 2024 on charges related to publications about the war (CPJ, 2024b; RFE/RL, 2024). Maria Ponomarenko, a journalist for RusNews, was sentenced to six years in prison in 2023 after reporting on the bombing of the Mariupol theater (CPJ, 2023; AMNESTY INTERNATIONAL, 2023). Ekaterina Barabash, a film critic for Republic, was placed under house arrest in 2025 after being charged over anti-war publications (CPJ, 2025b; RSF, 2025).

In this context, this work proposes Raven, a messaging application prototype focused on privacy under physical coercion. The proposal does not claim absolute security. Instead, it demonstrates a design approach centered on exposure reduction, plausible deniability, and the separation between a real environment and a decoy environment. The objective is to present the problem, describe the proposed solution, and document the current state of the local MVP developed for academic demonstration purposes.

MATERIALS AND METHODS

The adopted methodology was divided into four stages: problem identification, threat model definition, solution modeling, and implementation of a local MVP. The problem identification stage considered situations in which the user has limited

control over the device, especially in-person situations in which a phone may be demanded, unlocked, and inspected. From this perspective, the threat model assumes an adversary with temporary access to an unlocked device, capable of checking applications, recent conversations, and visible signs of hidden content.

The solution was modeled around three main flows. The first is normal access, in which a primary password opens the user's real environment. The second is access through a secondary password, which opens a fake account with simulated conversations and a coherent visual appearance, aiming to reduce suspicion during superficial inspection. The third is an emergency mode, represented in the prototype as a simulated blocking or cleaning action, without real data destruction at this stage.

The current prototype was developed in Flutter, prioritizing visual presentation and navigation between screens. It includes a splash screen with Raven's identity, an authentication screen with separate routes for the real password, fake password, and emergency mode, a conversation list, a chat screen with mock messages, a security tab explaining the features, and a profile tab. Since this is a local MVP, it does not yet include a functional backend, real message exchange, online registration, or operational end-to-end encryption.

For future development, the proposed architecture separates the user interface from the sensitive core. The interface may remain in Flutter, while the security core may be implemented in Rust and be responsible for cryptographic operations, key derivation, message packaging, and local access rules. A future backend, also potentially implemented in Rust, should act as an intermediary server for encrypted messages, avoiding access to message content and minimizing unnecessary logs.

RESULTS AND DISCUSSION

The result obtained so far is a navigable prototype that demonstrates Raven's central idea. Figure 1 presents a screen montage of the main MVP presentation, including the problem contextualization, proposed solution, prototype state, demonstration flow, differentials, and next steps. The implementation focused on communicating the proposal clearly during a presentation: showing that the project's security is not limited to message encryption, but also to how the application behaves when the user is under physical coercion.

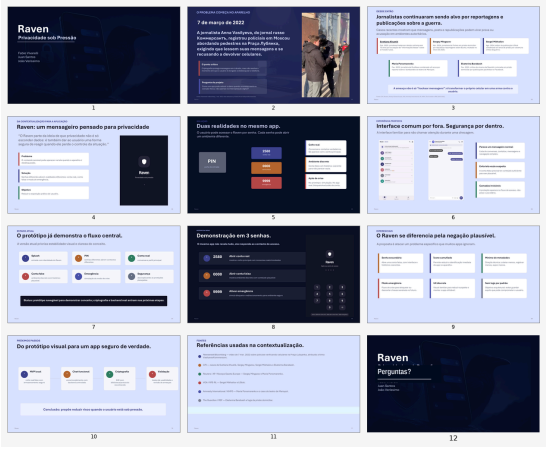


Figure 1. Screen montage of the Raven MVP presentation.

Source: Prepared by the authors (2026).

At its current stage, Raven has five demonstrable elements: primary password, secondary password, fake environment, simulated emergency mode, and conversation screens. For future versions, the main pending components include real chat between users, a synchronization backend, end-to-end encryption, encrypted local storage, and stronger metadata minimization mechanisms.

The prototype's main contribution is to demonstrate the concept of plausible deniability applied to the interface. In many messaging applications, the complete absence of content may itself create suspicion. Raven therefore proposes that the secondary password should open a fake environment that is visually consistent and less conspicuous. Even so, this mechanism does not eliminate risk: a trained adversary, or one with enough time and forensic resources, may identify inconsistencies, backups, notifications, residual files, or usage patterns.

Another relevant issue is the difference between content encryption and metadata protection. Even if future messages are encrypted, a server may still observe time patterns, traffic volume, contact frequency, and connection behavior. Therefore, Raven should be described as pursuing metadata minimization, not total metadata absence. Future development should consider encrypted local storage, minimal logging policies, discreet notifications, and a backend that only relays encrypted content.

There is also an ethical and personal safety limitation: poorly designed emergency features may increase the user's risk if an adversary notices that information was hidden or deleted. For this reason, the current MVP simulates emergency mode only as a concept, without implementing real data destruction. Safer future approaches should prioritize blocking, profile separation, and reduction of visible

exposure, while making clear that the system does not replace legal guidance, operational security, or field risk assessment.

CONCLUSION

Raven was conceived as a messaging application prototype focused on privacy under physical coercion. The developed local MVP demonstrates the central proposal through a primary password, a secondary password with a fake environment, a simulated emergency mode, and mock conversation screens. Although it does not yet include a backend, real communication, or end-to-end encryption, the prototype provides a basis for presenting the problem, evaluating the interaction flow, and discussing security limitations in scenarios of in-person surveillance.

As future work, the system should evolve toward an architecture with a Flutter interface, a Rust-based security core, encrypted local storage, and a backend for relaying encrypted messages. In addition, usability tests, a more formal threat analysis, and careful evaluation of the risks associated with plausible deniability in real coercion scenarios should be conducted.

ACKNOWLEDGMENTS

The authors thank the Federal Institute of Education, Science and Technology of São Paulo for the learning environment and for encouraging interdisciplinary projects involving technology, security, and society.

REFERENCES

AMNESTY INTERNATIONAL. Russia: Journalist Maria Ponomarenko sentenced to six years in penal colony over Ukraine bombing post. 2023. Available at: https://www.amnesty.org/en/latest/news/2023/02/russia-journalist-maria-ponomarenko-sentenced-to-six-years-in-penal-colony-over-ukraine-bombing-post/. Accessed on: May 26, 2026.

BUSINESS INSIDER. Russian police are demanding to read people's text messages, reporter says. 2022. Available at: https://www.businessinsider.com/russian-police-are-demanding-to-read-peoples-text-messages-reporter-2022-3. Accessed on: May 26, 2026.

COMMITTEE TO PROTECT JOURNALISTS (CPJ). Russian journalist Maria Ponomarenko sentenced to 6 years in prison. 2023. Available at: https://cpj.org/tags/maria-ponomarenko/. Accessed on: May 26, 2026.

COMMITTEE TO PROTECT JOURNALISTS (CPJ). Russia puts Forbes journalist under house arrest, detains 2 others. 2024a. Available at: https://cpj.org/2024/05/russia-puts-forbes-journalist-under-house-arrest-detains-2-others/. Accessed on: May 26, 2026.

COMMITTEE TO PROTECT JOURNALISTS (CPJ). Russian journalist Sergey Mikhaylov sentenced to 8 years in prison. 2024b. Available at: https://cpj.org/2024/08/russian-journalist-sergey-mikhaylov-sentenced-to-8-years-in-prison/. Accessed on: May 26, 2026.

COMMITTEE TO PROTECT JOURNALISTS (CPJ). Russia detains journalist Svetlana Khustik for fake news about Ukraine war. 2025a. Available at: https://cpj.org/2025/10/russia-detains-journalist-svetlana-khustik-for-fake-news-about-ukraine-war/. Accessed on: May 26, 2026.

COMMITTEE TO PROTECT JOURNALISTS (CPJ). Russia puts journalist under house arrest for fake news about Ukraine war. 2025b. Available at: https://cpj.org/2025/02/russia-puts-journalist-under-house-arrest-for-fake-news-about-ukraine-war/. Accessed on: May 26, 2026.

INTERNATIONAL PRESS INSTITUTE (IPI). Forbes Russia journalist detained for alleged fake news on Bucha. 2025. Available at: https://ipi.media/alerts/forbes-russia-journalist-detained-for-alleged-fake-news-on-bucha/. Accessed on: May 26, 2026.

NEWSWEEK. Video shows Russian police allegedly stopping people to screen phones. 2022. Available at: https://www.newsweek.com/video-shows-russian-police-allegedly-stopping-people-screen-phones-1685502. Accessed on: May 26, 2026.

RADIO FREE EUROPE/RADIO LIBERTY (RFE/RL). Siberian journalist gets 8 years in prison over articles about Ukraine war. 2024. Available at: https://www.rferl.org/a/siberia-sergei-mikhailov-listok-newspaper-prison-term-war-ukraine/33099419.html. Accessed on: May 26, 2026.

REPORTERS WITHOUT BORDERS (RSF). RSF exfiltrates Ekaterina Barabash: the Russian journalist's escape from Moscow to Paris. 2025. Available at: https://rsf.org/en/rsf-exfiltrates-ekaterina-barabash-russian-journalist-s-escape-moscow-paris. Accessed on: May 26, 2026.